(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 December 2003 (04.12.2003)

PCT

(10) International Publication Number
WO 03/101128 A1

(51) International Patent Classification[7]: H04Q 7/20, H04M 3/42

(21) International Application Number: PCT/EP03/50110

(22) International Filing Date: 16 April 2003 (16.04.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0212198.6 28 May 2002 (28.05.2002) GB

(71) Applicants *(for all designated States except US)*: **MOTOROLA INC** [US/US]; 1303 E.Algonquin Road, Schaumburg, IL 60196 (US). **MOTOROLA LIMITED** [GB/GB]; Jays Close, Viables Industrial Estate, Basingstoke, Hampshire RG22 4PD (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **KRAMER, David** [IL/IL]; Mishol Ha'rakefet 2, 76201 Ginot-Shomron (IL). **BAR-ON, David** [IL/IL]; Paldi 1, 76248 Rehovot (IL). **URS, Kamala, Diane** [US/US]; 861 Tallgrass Drive, Bartlett, IL 60103 (US). **BALLA, Chantal** [IL/IL]; Vardia 71, 34657 Haifa (IL).

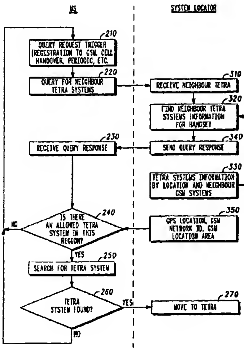
(74) Agent: **MCCORMACK, Derek, James**; Motorola European Intellectual, Property Operations, Midpoint, Alencon Link, Basingstoke, Hampshire RG21 7PL (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

[Continued on next page]

(54) Title: WIRELESS COMMUNICATION SYSTEM ARCHITECTURE, MOBILE STATION AND METHOD



200

(57) Abstract: A mobile station (172) is operable in at least a first wireless communication system (123) and in a second wireless communication system (173). The mobile station is operable to send to a System Locator (155) a query signal requesting the System Locator to provide information relating to connectivity of the mobile station with the first system, wherein the System Locator is accessible via the second system and the mobile station is operable to send said query signal during a period when it is connected by wireless to said second system. The first system may for example be a TETRA system and the second system may for example be a GSM system. A wireless communication architecture of communication systems in which the mobile station may be used and a System Locator for use in such architechture are also described.

WO 03/101128 A1

SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WIRELESS COMMUNICATION SYSTEM ARCHITECTURE, MOBILE STATION AND METHOD

Field of the Invention

This invention relates to a wireless communication system architechture, mobile station for use therein and communication method. In particular, it relates to the transmittal of information relating to wireless system location and connectivity.

Background of the Invention

Wireless communications systems, for example cellular telephony or private mobile radio communications systems, typically provide for radio telecommunication links to be arranged between a plurality of base transceiver stations (BTSs) and a plurality of subscriber units, often termed mobile stations (MSs). The term 'mobile station' generally includes both hand-portable and vehicular mounted radio units for transmission and receipt of radio communications of speech, data, video etc information.

Wireless communications systems are distinguished over fixed communications systems, such as the public switched telephone networks (PSTN), principally in that mobile stations move between service providers (and/or different BTS) and in

doing so encounter varying radio propagation environments.

In a wireless communication system, each BTS has associated with it a particular geographical coverage area (or cell). The coverage area is known as a serving cell and is defined by a particular range from the BTS within which the BTS can maintain acceptable communications with operating MSs. Often these cells overlap and combine to produce an expanded network coverage area. Furthermore, cells are often grouped into location areas for the purposes of tracking a MS within the coverage area whilst minimising location-updating signalling.

In the field of wireless communications, one of the most common complaints from mobile phone or radio customers is the unavailability of service in certain areas owing to lack of good radio frequency (RF) coverage, or lack of system coverage in large geographical areas such as coverage of a state. This is a problem even with MSs that support widely used networks such as the Global System for Mobile communications (GSM). This problem is more prevalent with MSs that support networks that are currently not as widely deployed, for example networks operating specifically for certain organisations, such as TETRA or iDEN™ systems which are usually owned and operated for the benefit of the particular user organisations.

One mechanism that has been chosen by some network operators and MS manufacturers to address the coverage problem is to provide dual-mode MSs to support two modes of operation. For example, a basic mode may be for the MS to communicate in a TETRA mode of operation, where direct (radio to radio) mode of communication is supported in addition to cellular operation using the network infrastructure in the TETRA network. As a secondary mode of operation, when the user is in an area where there is no TETRA network coverage available, the MS may be re-configured to operate directly as a cellular phone on a GSM network.

When operating in a GSM mode, the user and the network operator may be interested in returning the user to another network such as a TETRA network or a an integrated digital enhanced network (iDEN ™) network, as soon as possible, e.g. in order to use the dedicated communication services available.

The Applicant and its subsidiaries produce and market MSs, such as some iDEN MS models that support both an iDEN communication format and a GSM communication format. However, the switching between iDEN and GSM networks is only effected by the user when (s)he recognises that such switching is possible, and manually switches the mode of operation. Alternatively, such switching may occur automatically and without user control, as a user

loses coverage on one network and re-registers automatically on the other network.

In particular, a significant disadvantage with a manual switching approach is that the user will be unaware of whether (s)he is within the coverage range of the alternative communication system. The user may switch modes manually and intermittently so that the terminal can search for an alternative network, if the user suspects there might be an alternative network in the area. This is a tedious operation for the user, with no guarantee of successfully finding an alternative network. Additionally, such a manual approach also causes a communication downtime for the user, whilst the terminal is leaving the existing network and searching (perhaps unsuccessfully) for an alternative network. For the abovementioned situation of a dual-mode GSM-TETRA MS, it is likely to take up to several minutes to search for a TETRA network whilst operating in a GSM mode, with no guarantee of success. During this time, the subscriber unit is, as indicated, effectively unusable.

Another solution used in dual-mode wireless communication units is the concept of 'dual watch'. A dual watch approach, as described in GB-A-2287612, applicant Motorola Ltd., enables a MS to monitor, periodically, a second network, whilst still communicating on a first network. However, due to

differences in, for example, frequency bands, modulation schemes, limits on transmit power, bandwidth restrictions, etc. between dissimilar networks, it is very difficult to implement such a dual watch mechanism.

Clearly, an improved dual-watch mechanism can be implemented using two independent receivers (and potentially two independent transmitters) in a single subscriber communication unit, one receiver configured for each communication system. However, the provision of a dual receiver solution, to constantly monitor the other network, is relatively expensive.

A need therefore exists for an improved mechanism for selecting, and ultimately switching between, wireless communication systems wherein the abovementioned disadvantages may be alleviated.

Summary of Invention

According to the present invention in a first aspect there is provided a mobile station operable in at least a first wireless communication system and in a second wireless communication system, the mobile station being operable to send to a System Locator a query signal requesting the System Locator to provide information relating to connectivity of the mobile station with the first system, wherein the System Locator is accessible via the second system

and the mobile station is operable to send said query signal during a period when it is connected by wireless to said second system.

The mobile station may be operable to send to the System Locator via the second system one or more signals including information relating to current location of the mobile station for use by the System Locator in providing connectivity information relating to the first system. The information relating to current location of the mobile station may be included in or in connection with the query signal.

The mobile station may be operable to send the query signal periodically. Alternatively, or in addition, the mobile staion may be operable to send the query signal when a predetermined event occurs or has occurred. The pre-determined event may comprise one or more of:

(i) registering on said second wireless communication system,

(ii) performing a cell handover,

(iii) roaming to a new location area.

The mobile station according to the first aspect may be operable to send said query signal by text or data message signalling. The query signal may include an identity address of the System Locator by which the signal can be routed to reach the System Locator via the second system

The mobile station according to the first aspectmay be operable to receive via the second system a signal sent from the System Locator including information relating to connectivity with the first system. The information may indicate whether the mobile station is within communication coverage range of the first system. The information may include information about at least one operational parameter of the first system. The information may include, in relation to the first system, information including one or more of: one or more radio frequencies used, a duplex frequency offset, a list of control channel frequencies, at least one timing parameter, and a geographical boundary of coverage of the first wireless communication system.

The mobile station may be operable to receive said parameter information when the System Locator determines that the mobile station is within communication coverage range of the first system.

The mobile station may be operable to send successive query signals via the second system to the system Locator and to receive in response to such query signals response signals in which the information received from the System Locator via the second system is updated for each response signal, recognising movements in location of the mobile station.

The mobile station may be operable to use the received information to determine whether to search for the first system. The mobile station may be operable following receipt of a signal from the System Locator via the second system indicating that the mobile station is within wireless communication coverage range of the first system to switch its operation to wireless communication with the first system.

According to the present invention in a second aspect there is provided a wireless communication architecture including a first wireless communication system, a second wireless communication system, a System Locator accessible by the second system and at least one mobile station operable alternatively in either the first system or the second system, wherein the mobile station is a mobile station according to the first aspect.

In the wireless communication architecture according to the second aspect, the first and second systems may be systems using different communication protocols.The first and second systems may be mobile communication network systems. One of the first and second systems may for example be a system operating according to GSM standards. The other one of the first and second systems may for example be a system operating according to TETRA standards. Alternatively, one system may be a GSM system and

the other system may be a known IS136 or a known CDMA system.

The System Locator may be included within a management control function in said first wireless communication system or said second wireless communication system. It may comprise a programmable digital signal processorin any of the forms known in the art. The System Locator may be operable to store operational information relating to said first wireless communication system, and optionally relating to said second wireless communication system.

According to the present invention there is provided a System Locator for use in the architechture according to the second aspect. The System Locator may be operable to provide information to at least one dual-mode mobile station connected by wireless to the second wireless communication system and capable of operating in the first wireless communication system, such that said information relates to connectivity of the mobile station with the first sytem. The System Locator may be operable to operable to generate and provide the connectivity information using information relating to the current location of the mobile station. The information relating to the current location of the mobile station may be information sent in or in connection with a query signal by the mobile station. The System Locator may be operable to send

to the at least one mobile station via the second system information relating to at least one operational parameter of said first wireless communication system or use by the at least one mobile station in searching for and/or switching its operation to said first wireless communication system.

According to the present invention in a fourth aspect there is provided a method of selecting a wireless communication system in a wireless communication architecture that includes a first wireless communication system and a second wireless communication system, the method comprising the step of:

operating at least one dual-mode mobile station unit by wireless connection in said second wireless communication system; and

determining a location of said at least one mobile station;

the method being characterised by the step of:

providing information relating connectivity of said mobile station with said first system, the information including optionally at least one operational parameter of said first wireless communication system, said information being provided to said at least one mobile station via said second wireless communication system.

By providing operational information about a neighbouring communication system or network in the

manner of the invention, an MS may beneficially limit the time taken in searching for and registering on alternative networks. Preferably, the operational information is received from a System Locator in the MS's home network (e.g. a TETRA network), access via the network it is currently operating in (e.g. a GSM network).

Preferably, the dual-mode MS may query its home network about possible alternative networks in the area where the MS is currently operating. When the query includes information about the MS's geographic location, or information of the network it is currently operating on, the alternative network response can be tailored for the MS's current location.

The network currently supporting communication to/from a MS aids the MS in contacting the System Locator to determine whether or not the MS should search for and/or to attempt to switch networks. This saves the MS from the need to leave the current network in order to perform random searches for an alternative network.

The potential speed of such a method of finding a switching to another system, e.g. a home network, is of considerable practical benefit to the user.

A particular implementation of the present invention is that whilst operating on a GSM system, the MS

will be able to query its home TETRA system as to whether or not there is TETRA coverage in the area were the MS is located. The operational information is preferably communicated using short messages (e.g. a short message service (SMS) on GSM and/or a supplementary data service (SDS) on TETRA). Other methods, such as Internet Protocol (IP) using packet data transfer through the Internet, can also be used.

GB-A-2313257 discloses a "Bulletin Board System" (BBS) to provide identification of usable radio-systems in the area where a radio is located. However, the arrangement described requires the existence of a separate radio-system, the "Common Communications Systems" (CCS). Through the CCS the radio receives information from the BBS. However, unlike the invention, the radio does not receive the information while being connected by wireless to a usable communication system, one which provides communication with other radios, and therefore while working actively on one of the communication systems. Thus the arrangement of GB-A-2313257 requires the radio to interface separately with a radio-system (the CCS) just for the purpose of obtaining information about the usable systems available. The information about the systems available is not updated while the radio is currently working in a particular communication system because the radio is not then connected to the CCS and there is no actual or contemplated use

of the facilities which can be provided by such a working system (e.g. use of SMS, Packet Data, IP routing of messages etc. available in GSM and TETRA systems). The radio does not look for other systems whilst continuing to work on the current working system.

Exemplary embodiments of the present invention will now be described, with reference to the accompanying drawings, in which:

Brief Description of the Drawings

FIG. 1 is a block schematic diagram (also reflecting coverage area) of a wireless communication architecture adapted in accordance with an embodiment of the present invention; and

FIG. 2 is a flowchart of events and states of a mobile station and System Locator performing a method of selecting a wireless communication system, in accordance with an embodiment of the present invention.

Detailed Description of Embodiments of the Invention

Although the following embodiment of the present invention is described with reference to interaction between a TETRA system and a GSM system, it is within the contemplation of the invention that the

inventive concepts described herein can be applied to any two or more wireless communication systems.

Referring first to FIG. 1, a schematic diagram 100 of a a system architechture comprising a combination of communication systems is shown. The diagram includes a trunked radio communication system, supporting a TETRA (TErrestrial Trunked Radio) air-interface protocol, shown in outline, adapted in accordance with an embodiment of the invention. The European Telecommunications Standards Institute (ETSI) has defined the TETRA air-interface. Generally, the air-interface protocol is administered from base transceiver sites that are geographically spaced apart - one base site supporting a cell (or, for example, sectors of a cell) - providing a defined TETRA coverage area 123. A second cellular radio telephone system, for example a Global System for Mobile (GSM) communications, is shown, in the vicinity of the TETRA system with coverage area 173. The GSM air-interface has also been defined by ETSI.

In the TETRA system, a plurality of subscriber units, such as a mixture of MSs 112-116 and fixed terminals (not shown), communicate over the selected air-interface 118-120 with a plurality of base transceiver stations (BTS) 122-132. A limited number of MSs 112-116 and BTSs 122-132 are shown for clarity purposes only.

The system infrastructure in a TETRA system is generally referred to as a switching and management infrastructure (SwMI) 110, which substantially contains all of the system elements apart from the mobile units. The BTSs 122-132 may be connected to a conventional public-switched telephone network (PSTN) 134 through base station controllers (BSCs) 136-140 and mobile switching centres (MSCs) 142-144.

Each BTS 122-132 is principally designed to serve its primary cell, with each BTS 122-132 containing one or more transceivers. The BTSs 122-132 communicate 156-166 with the rest of the trunking system infrastructure via a frame relay interface 168.

Each BSC 136-140 may control one or more BTSs 122-132, with BSCs 136-140 generally interconnected through MSCs 142-144. Each BSC 136-140 is therefore able to communicate with one another, if desired, to pass system administration information therebetween, with BSCs 136-140 responsible for establishing and maintaining control channel and traffic channels to serviceable MSs 112-116 affiliated therewith. The interconnection of BSCs 136-140 therefore allows the trunked radio (or cellular phone) communication system to support handover of the MSs 112-116 between cells.

Each MSC 142-144 provides a gateway to the PSTN 134 and, although not shown, they can provide an

interface to a packet data network, e.g. Internet, through some manner of Packet Data Gateway. MSCs 142-144 are interconnected through an operations and management centre (OMC) 146 that administers general control of the trunked radio system 100, as will be understood by those skilled in the art. The various system elements, such as BSCs 136-138 and OMC 146 include control logic 148-152 with the various system elements usually having associated memory. The memory typically stores historically compiled operational data as well as in-call data, system information and control algorithms.

In a preferred embodiment of the present invention, the OMC 146 has been adapted to include a System Locator 155. The System Locator 155 provides information relating to one or more alternative systems offering service or coverage within the geographical areas that are also supported by the TETRA system. In the preferred embodiment of the present invention, the System Locator 155 within the OMC 146 contains operational information relating to the GSM system, supporting GSM communications in coverage area 173.

In accordance with the preferred embodiment of the present invention, the System Locator 155 in the TETRA system is configured to inform the MS 172 operating in the GSM system 173 whether or not there is a TETRA system in the area it is located. Preferably, the System Locator 155 also informs the

MS 172 of the radio frequencies the TETRA network uses. This enables the MS 172 to search automatically for a TETRA network only when there is a good chance that there is a TETRA network in its operating area.

When the MS 172 recognises there is a TETRA network in the area, the MS 172 is preferably restricted to search only a limited range of TETRA radio frequencies. The provision of such radio frequency information to MS 172 greatly reduces the amount of time the MS 172 is out of GSM service in searching for a TETRA system. Furthermore, the time it takes to typically find a TETRA network is also reduced.

It is within the contemplation of the invention that the System Locator 155 may be supported in one or more of the communication systems, for example the GSM and/or TETRA communication system of FIG. 1. Alternatively, it is envisaged that the System Locator may be located distal from, but operably coupled to, both wireless communication systems.

The System Locator 155 preferably includes a database that stores locations of known TETRA systems. It is envisaged that the System Locator 155 may also store information on known GSM systems, which is advantageous in situations, for example, where the System Locator 155 was a stand-alone device and operably coupled to both the TETRA and GSM networks.

In addition to the RF channels used by a network, the database preferably includes information on:

(i) Any duplex frequency offset used,

(ii) A list of Control Channel frequencies used by the TETRA networks, and/or

(iii) The geographical boundaries of the TETRA networks if the MS provides geographic location information.

The OMC 146 of the TETRA system is preferably operably coupled to the OMC 176 of the GSM system, at least via the System Locator 155, so that information, such as operating radio frequencies, system timing parameters, etc. relating to both systems can be passed therebetween.

In a similar manner to the TETRA system, the GSM system may include an OMC 176 that is operably coupled to a BTS 174. The BTS supports GSM communication to/from MS 172. The other infrastructure elements of the GSM system, which roughly follow the same principles and architecture of the TETRA system, are not shown for clarity purposes only.

In an alternative embodiment of the present invention, the GSM network broadcasts TETRA-related information to the GSM MSs operating within its network, and vice versa. This solution may require cooperation of both the GSM and TETRA operators to

agree to communicate the necessary information to communication units operating in their respective cells. It is appreciated that this alternative embodiment would also likely need amendments to the GSM and/or TETRA standard, in order to facilitate the transmission of such messages.

Referring now to FIG. 2, a flowchart 200 of events and states of the MS 172 and System Locator 155 of FIG. 1, when the MS is searching for a TETRA system whilst operating on, say, a GSM system, is shown. When operating in a GSM mode, the dual-mode (GSM-TETRA) MS (for example, MS 172) periodically sends a "Neighbour System Query" short message service (SMS) message to a known ID (phone number) on the TETRA network, as shown in step 220.

The preferred embodiment of the present invention utilises the existing message structure of GSM short message service (SMS) and/or TETRA supplementary data service (SDS) for interface between the MS and the System Locator. However, it is within the contemplation of the invention that other message structure and formats could be used to enable the users and systems to benefit from the inventive concepts described herein.

For example, it is envisaged that the transfer of information may include the use of packet data transmissions to communicate with the System Locator

that contains the TETRA and/or GSM system information. Alternatively, the transfer of information may include the use of intelligent networking to trigger communication with the System Locator containing the TETRA and/or GSM system information. The System Locator may then respond via a mobile terminated SMS message.

In contrast to periodic SMS messages being sent to the System Locator 155 of the TETRA system, for example once per hour, it is envisaged that the system information requests may be event-driven as shown in step 210. It is envisaged that such events that could trigger the query, may include:

(i) Registering on a GSM system,

(ii) Cell handover,

(iii) Upon roaming to a new Location Area in the GSM network, etc.

In addition, it is envisaged that any combination of two or more of the above events could be employed at different times or under different circumstances, for example, only on network registration when there is no TETRA system in the area.

Furthermore, it is envisaged that when the home location register (HLR) of the MS's TETRA home network receives a message that the MS is registering on a new GSM network, the System Locator may transmit TETRA system information to the MS, without the need for the MS to request it.

Any query message from the MS may contain various forms of information, as shown in step 350. It is envisaged that such information may include, for example:

(i) Information relating to the current location of the MS supplied, say by a GPS indication,

(ii) A GSM Network ID, and/or

(iii) A GSM Location Area (LA).

The message will be routed to the TETRA network through the network's inter-system interface (ISI).

On the TETRA network, the message will be routed to a System Locator device, as in step 310. It is envisaged that step 310 may potentially include translation to a TETRA SDS message.

If the MS provided geographic location, the System Locator can accurately determine whether the MS is in the coverage area of a TETRA network. If GSM Network ID and/or LA are provided, as in step 330, the System Locator can determine the potential TETRA networks that the MS can search for.

The System Locator then sends a query response to the MS, using, say, a SMS GSM message (or TETRA SDS that will be translated to SMS before being routed to the GSM network), as shown in step 340. The message indicates whether or not there is a TETRA network in the area. If there is a TETRA network in

the area, the message also preferably includes information about the radio frequency (RF) channels and/or timing used by the TETRA network(s).

It is envisaged that the System Locator may also send the MS information on the Network IDs of the TETRA networks in the MS's area. In this manner, the MS could choose not to leave the GSM system, and search for a TETRA network, if it knows that none of the TETRA networks are allowed or preferred networks.

It is further envisaged that, where the MS provides geographic location information, the System Locator may also send the MS information on whether the MS is near a TETRA network, so that the MS may search for the network periodically, even before sending the next query, if it so wishes.

When receiving the query response in step 230, the MS determines whether it is in the coverage area of a TETRA network, as in step 240, based on the information received and its location (if known). If the MS determines that it may be in such a coverage area, it will search for the one or more TETRA systems, as shown in step 250. If a TETRA system is found in step 260, the MS may leave the GSM system and register on the TETRA system, as shown in step 270.

If the location determination is based on the GSM Network identifier (mobile network identity (MNI)) and other information such as Location Area from step 350, then it is envisaged that the database may include, for each TETRA network, a list of GSM networks that are active in the coverage area of the TETRA network.

The preferred configuration of operably coupling the System Locator to the alternate network (e.g. GSM) via an OMC link is shown as an example only. It is envisaged that a further example of a connection from the System Locator to the alternate network may be through a visitor location register (VLR)/ home location register (HLR) interface.

In an alternative configuration, the System Locator may be connected to the alternate network via a short message service centre (SMSC) routing the messages directly to the System Locator, for example using an Internet protocol (IP)-based structure. A skilled artisan would appreciate that other network configurations could also benefit from the inventive concepts described herein. Additionally, the two or more wireless communication systems may be adjacent one another, overlapping, or substantially contained within one another in a pico-cell to micro-cell to macro-cell manner. As such, the wireless communication systems only need to be in the vicinity of one another to facilitate a potential hand-over of wireless communications therebetween.

The inventive concepts find particular application in use between dissimilar communication systems, for example a GSM cellular communication system and a private mobile radio communication system. It is within the contemplation of the invention that such routing of neighbouring system information may be utilised in any other wireless communication system, such as a wireless local area networks (WLANs), a third generation partnership project (3GPP) communication system, etc.

Although the aforementioned inventive concepts have been described with reference to interaction between TETRA and GSM systems, it is within the contemplation of the present invention that such concepts can be applied to other types of wireless cell-based communication systems. For example, an MS operating on a GSM system may receive information on neighbouring iDEN™ systems and vice versa; an MS operating in IS-136 system may receive information on neighbouring GSM systems and vice versa; an MS operating on a foreign TETRA system may receive information on its Home TETRA system.

Although the invention preferably utilises the GSM SMS and TETRA SDS mechanism to transfer messages between the MS and the System Locator, it is envisaged that other mechanisms may be used. For systems other then TETRA and GSM, it is envisaged

that their particular short message mechanism(s) may replace the GSM SMS or TETRA SDS message formats. In addition, the interface between the two or more systems may be implemented using other methods, such as IP messages, where the System Locator can be connected to the Internet. Advantageously, if an Internet interface is used, no agreement between the system operators is required.

Furthermore, it is envisaged that a third party may provide a stand-alone System Locator that can be operably coupled to any two or more neighbouring (or overlapping) wireless communication systems. However, such an implementation would need to consider the security aspects associated with implementing such a standard interface to multiple wireless communication systems.

It will be understood that the wireless communication architecture and method of selecting a wireless communication system, as described above, provides at least the following advantages:

(i) An MS may limit the time taken in searching and registering on alternative networks by receiving information about alternative networks from, say, the MS's home network, via the network it is currently operating in.

(ii) By including Network IDs (MNIs) in the communication to the MS, the MS can check whether it has received authorisation to operate on the alternative networks in its current location, without first needing to start a registration process with, or connect to, the alternative network.

(iii) A mechanism is provided for a dual-mode MS to query, say, its home network about possible alternative networks in the area where the MS is currently operating. When the query includes the MS's geographic location, or information of the network it is currently operating on, the alternative network response can be tailored for the MS's current location.

(iv) The network currently supporting communication to/from a MS aids the MS in determining whether or not to attempt to switch between systems. This prevents the MS from needing to leave the current network in order to perform random searches for an alternative network.

(v) A variety of message formats may be used to inform the MS of alternative systems, for example, SMS messages to interface with the System Locator when it is located within the TETRA system or using Packet Data when it is communicating via, say, the Internet.

Thus, an improved mechanism for monitoring, and ultimately switching between, wireless cellular-based communication systems has been described wherein the disadvantages associated with prior art arrangements have been substantially alleviated.

Claims

1. A mobile station (172) operable in at least a first wireless communication system (123) and in a second wireless communication system (173), the mobile station being operable to send to a System Locator (155) a query signal requesting the System Locator to provide information relating to connectivity of the mobile station with the first sytem, wherein the System Locator is accessible via the second system and the mobile station is operable to send said query signal during a period when it is connected by wireless to said second system.

2. A mobile station according to claim 1 and wherein the mobile station is operable to send to the System Locator via the second system one or more signals including information relating to current location of the mobile station.

3. A mobile station according to claim 2 and wherein the information relating to current location of the mobile station is included in or in connection with the query signal.

4. A mobile station according to any one of the preceding claims and wherein the mobile station is operable to send the query signal periodically.

5. A mobile staion according to any one of the preceding claims and wherein the mobile station is

operable to send the query signal when a predetermined event occurs or has occurred.

6. A mobile staion according to claim 5, wherein the pre-determined event comprises one or more of:

(i) registering on said second wireless communication system (173),

(ii) performing a cell handover,

(iii) roaming to a new location area.

7. A mobile station according to any one of the preceding claims and which is operable to send said query signal by text or data message signalling.

8. A mobile staion according to any one of the preceding claims and wherein the mobile station is operable to produce a signal including an identity address of the System Locator and to send the signal to the System Locator via the second system.

9. A mobile station according any one of the preceding claims and wherein the mobile station is operable to receive via the second system a signal sent from the System Locator including information relating to connectivity with the first system.

10. A mobile station according to claim 9 and wherein the mobile station is operable to receive via the second system from the System Locator a signal indicating whether the mobile station is within communication coverage range of the first system.

11. A mobile station according to claim 9 or claim 10 and wherein the mobile station is operable to receive signals including information about at least one operational parameter of the first system.

12. A mobile station according to claim 11 and wherein the mobile station is operable to receive, in relation to the first system, information including one or more of: one or more radio frequencies used, a duplex frequency offset, a list of control channel frequencies, at least one timing parameter, and a geographical boundary of coverage of the first wireless communication system (123).

13. A mobile station according to claim 12 and wherein the mobile station is operable to receive said information when the System Locator determines that the mobile station is within communication coverage range of the first system.

14. A mobile station according to any one of claims 9 to 13 and wherein the mobile station is operable to send successive query signals via the second system to the system Locator and to receive in response to such query signals response signals in which the information received from the System Locator via the second system is updated for each response signal.

15. A mobile station according to any one of claims 9 to 14 and which is operable to use the received

information to determine whether to search for the first system.

16. A mobile station according to any one of claims 9 to 15 and wherein the mobile station is operable following receipt of a signal from the System Locator via the second system indicating that the mobile station is within wireless communication coverage range of the first system to switch its operation to wireless communication with the first system.

17. A wireless communication architecture (100) including a first wireless communication system (123), a second wireless communication system (173), a System Locator (155) accessible by the second system and at least one mobile station operable alternatively in either the first system or the second system, wherein the mobile station is a mobile station according to any one of claims 1 to 16.

18. A wireless communication architecture according to claim 17 wherein the first and second systems are systems using different communication protocols.

19. A wireless communication architecture according to claim 18 wherein the first and second systems are mobile communication network systems.

20. A wireless communication architecture according to any one of claims 17 to 19 and wherein one of the

first and second systems is a system operating according to GSM standards.

21. A wireless communication architecture according to any one of claims 17 to 20 and wherein one of the first and second systems is a system operating according to TETRA standards.

22. A wireless communication architechture (100) according to any one of claims 17 to 21 and wherein the System Locator is included within a management control function in said first wireless communication system (123) or said second wireless communication system (173).

23. A wireless communication architecture (100) according to any one of claims 16 to 22, wherein the System Locator (155) is operable to store operational information relating to said first wireless communication system (123), and optionally relating to said second wireless communication system (123).

24. A System Locator (155), operably coupled to a first wireless communication system (123) and a second wireless communication system (173), wherein the System Locator (155) is operable to provide information to at least one dual-mode mobile station (172) connected by wireless to the second wireless communication system and capable of operating in the first wireless communication system, such that said information relates to connectivity of the mobile station with the first sytem.

25. A System Locator according to claim 24 and which is operable to provide the connectivity information using information relating to the current location of the mobile station.

26. A System Locator according to claim 25 and wherein the information relating to the current location of the mobile station is information sent in or in connection with a query signal by the mobile station.

27. A System Locator according to any one of claims 24 to 26 and wherein the System Locator is operable to send to the mobile station via the second system information relating to at least one operational parameter (330) of said first wireless communication system (123) for use by the at least one mobile station (172) in searching for and/or switching its operation to said first wireless communication system (123).

28. A method of selecting a wireless communication system in a wireless communication architecture (100) that includes a first wireless communication system (123) supporting communications in the vicinity of a second wireless communication system (173), the method comprising the step of:

operating at least one dual-mode mobile station unit (172) by wireless connection in said second wireless communication system (173); and

determining a location of said at least one mobile station(172);

the method being characterised by the step of:

providing (340) information relating connectivity of said mobile station with said first system, the information including optionally at least one operational parameter (330) of said first wireless communication system (123), said information being provided to said at least one mobile station via said second wireless communication system (173).

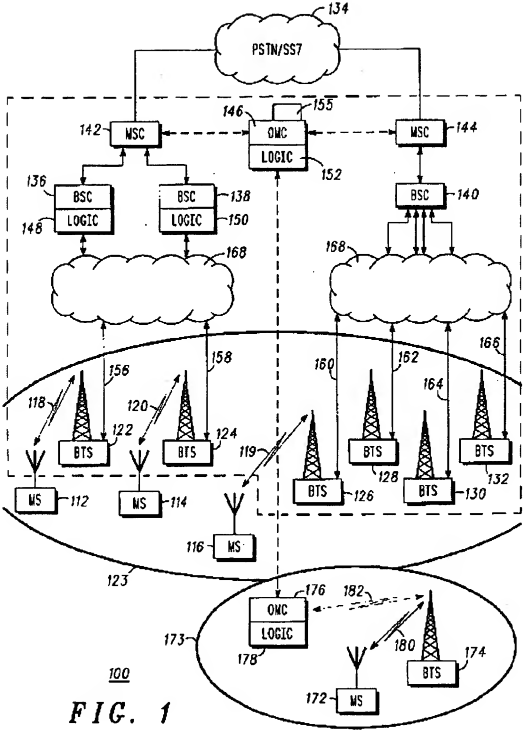

134
PSTN/SS7
146
155
142
MSC
OMC
LOGIC
MSC
144
152
136
BSC
LOGIC
148
BSC
LOGIC
138
150
BSC
140
168
168
156
158
160
162
164
166
118
120
122
124
BTS
BTS
119
BTS
BTS
BTS
BTS
126
128
130
132
MS
112
MS
114
MS
116
123
176
182
OMC
LOGIC
178
173
180
BTS
174
MS
172
100

FIG. 1

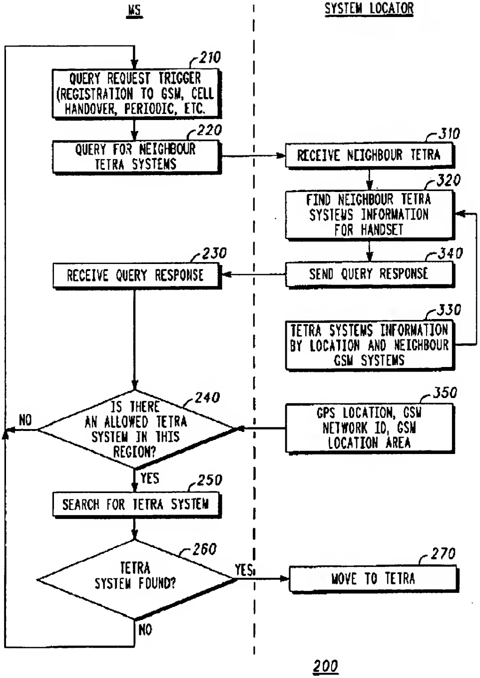

MS
SYSTEM LOCATOR
210
QUERY REQUEST TRIGGER (REGISTRATION TO GSM, CELL HANDOVER, PERIODIC, ETC.
220
QUERY FOR NEIGHBOUR TETRA SYSTEMS
310
RECEIVE NEIGHBOUR TETRA
320
FIND NEIGHBOUR TETRA SYSTEMS INFORMATION FOR HANDSET
230
RECEIVE QUERY RESPONSE
340
SEND QUERY RESPONSE
330
TETRA SYSTEMS INFORMATION BY LOCATION AND NEIGHBOUR GSM SYSTEMS
240
IS THERE AN ALLOWED TETRA SYSTEM IN THIS REGION?
NO
YES
350
GPS LOCATION, GSM NETWORK ID, GSM LOCATION AREA
250
SEARCH FOR TETRA SYSTEM
260
TETRA SYSTEM FOUND?
YES
NO
270
MOVE TO TETRA
200

FIG. 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/50110

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/20 H04M3/42

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 822 418 A (YACENDA MICHAEL W ET AL) 13 October 1998 (1998-10-13) column 1, line 20 -column 2, line 48 abstract	1-28
Y	US 5 924 040 A (TROMPOWER MICHAEL L) 13 July 1999 (1999-07-13) column 2, line 65 -column 4, line 35 abstract; figures 6,7	1-28
Y	US 6 006 096 A (TROMPOWER MICHAEL L) 21 December 1999 (1999-12-21) column 1, line 19 -column 5, line 64 abstract; figures 8-10	1-28

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 July 2003	25. 07. 2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	BEHROZ MORADI/JA A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/50110

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6 075 458 A (GRAZZINI ANDREA J ET AL) 13 June 2000 (2000-06-13) column 1, line 8 -column 2, line 17 abstract ---	1-28
Y	EP 0 756 430 A (AT & T CORP) 29 January 1997 (1997-01-29) page 2 -page 3 abstract; figures 13-16 -----	1-28

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 03/50110

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
US 5822418	A	13-10-1998	US	5515426	A	07-05-1996
			AT	180370	T	15-06-1999
			AU	708573	B2	05-08-1999
			AU	1933995	A	11-09-1995
			CA	2184165	A1	31-08-1995
			DE	69509755	D1	24-06-1999
			DE	69509755	T2	27-01-2000
			EP	0748556	A1	18-12-1996
			ES	2132649	T3	16-08-1999
			WO	9523478	A1	31-08-1995
US 5924040	A	13-07-1999	US	6006096	A	21-12-1999
US 6006096	A	21-12-1999	US	5924040	A	13-07-1999
US 6075458	A	13-06-2000	US	5594425	A	14-01-1997
			US	6331825	B1	18-12-2001
EP 0756430	A	29-01-1997	US	5873048	A	16-02-1999
			EP	0756430	A2	29-01-1997
			JP	9121378	A	06-05-1997

An Architecture for Integrating CDMA2000 and 802.11 WLAN Networks

Hamid Syed Mahmood
Wireless Technology Labs
Nortel Networks
Ottawa, Canada
hmsyed@nortelnetworks.com

Bill Gage
Wireless Technology Labs
Nortel Networks
Ottawa, Canada
gageb@nortelnetworks.com

***Abstract*— Low cost, high speed wireless LAN networks can be integrated within the cellular coverage to provide hot spot coverage for high speed data services. This article presents a novel approach for integrating North American 3G cellular network and 802.11 wireless LAN networks. The inter-technology mobility is supported using the standard cdma2000 functions and signaling.**

Keywords: IEEE802.11, CDMA2000, mobility, hot spot, heterogenous networks

I. INTRODUCTION

The 3G cellular networks are designed to offer high speed access for mobile data users. However, the demand for bandwidth in the 3G cell is not uniform throughout the cell. Rather, it is clustered in hotspot areas such as airports, hotels, shopping malls, apartment buildings, Internet cafes etc. In addition, the availability of bandwidth in the 3G cell is not uniform throughout the cell. In general, higher bandwidths are only available close to the cell site while only lower bandwidths are available further from the cell site. Fading and obstructions further affect the availability of bandwidth at any point within the cell. IEEE 802.11 Wireless LAN (WLAN) is a short-radius radio technology that is gaining a tremendous momentum in the marketplace. The cellular operator can take advantage of this low cost, high speed technology to cover the hot spots and gaps in coverage within its cellular network. In such scenarios, the mobile wireless access network is expected to be heterogeneous in nature and may allow the mobile user to move between the 3G cellular to the WLAN coverage area and vice versa. However, neither the existing 3G cellular nor the WLAN standards provide an integrated network architecture to support seamless mobility of the user between the two technologies. An integrated network architecture to support 3G UMTS network and WLAN is presented in [1]. Some other related work on WLAN inter-operability can be found in [2, 3, 4]. In this article, we propose a novel architecture to allow seamless mobility between the North American 3G cellular standard (cdma2000) and 802.11 WLAN networks. This proposal reuses the standard cdma2000 functions and signalling messages to perform an inter-technology handover.

II. BACKGROUND

A. CDMA2000 Network

The 3rd generation North American wireless standard [5] is based on cdma2000 radio technology. It provides circuit-switched (CS) service for voice and the packet-switched (PS) service for data transport. The network between the mobile station and the base station controller (BSC) (including the base station BTS) forms the radio access part of the cdma2000 network (Figure 1). The packet network is represented by the R-P (radio-to-packet) interface between BSC and packet data serving node (PDSN). The generic encapsulation protocol (GRE) [18] is recommended for the R-P interface. A packet control function (PCF) at the BSC handles the packet signaling and data transfer between the radio and packet parts of the cdma2000 network. End-to-end packet data between the mobile station and the packet data serving node (PDSN) is transported through the Point-to-Point Protocol (PPP) [11].

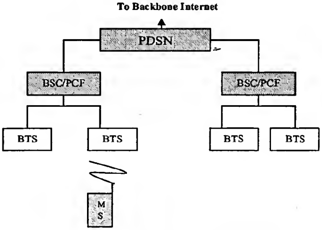


Figure 1. An Example of CDMA 2000 Network

B. 802.11 WLAN and IP over WLAN

The IEEE 802.11 WLAN [7, 8, 9] network is composed of a number of access points (APs) and the Mobile Stations (MS) accessing the WLAN network through one of the APs. A

number of APs can be interconnected through an IP routed network to form the WLAN IP network. An access router (AR) connects one or more APs to the IP access network. An access network gateway (ANG) connects the WLAN IP access network to the backbone Internet world, as shown in Figure 2.

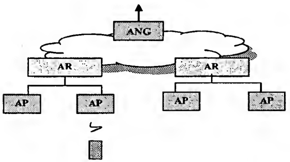


Figure 1. An Example of WLAN IP Network

A. *CDMA2000 and WLAN Integration: HotSpot Scenario*

A hotspot area is defined as a dense population of the users in a small area. An operator may have cellular coverage across these areas but it may want to provide lower cost, higher speed coverage to the users in the hot spot area. In this hot spot scenario, WLAN is used primarily for data connection only and it operates in conjunction with the cdma2000 cellular network. Users with dual-mode mobile devices can access the two networks. The devices have two network interfaces - one connects with the cellular network and the other with WLAN network. It is possible to use common billing and network authentication infrastructure as well as common connectivity to the Internet.

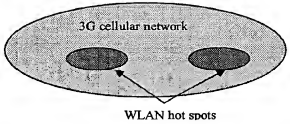


Figure 2. Hot Spot Coverage with Integrated Cellular and WLAN networks

III. INTEGRATED NETWORK ARCHITECTURE

The Integrated architecture proposes re-using the PDSN of cdma2000 network to forward the WLAN traffic as well. A proxy packet control function introduced at ANG replicates the PCF function of cdma2000 BSC. In this way, it acts as a gateway between the WLAN IP network and the PDSN. The WLAN access network appears as another cdma2000 network to the PDSN (refer Figure 4).

The integrated network architecture re-uses as much as possible from the existing cdma2000 and 802.11 WLAN protocols. Hence, no changes are required to the standard cdma2000 PS service or to the standard 802.11 AP. However, in order to achieve an integrated network operation supporting seamless mobility between the two technologies, the following new functions are introduced.

- The mobile station must have both a WLAN and a cdma2000 radio interface. It makes intelligent decisions on which radio technology to use at any moment, and diverts the PPP frames to the selected radio interface.
- A proxy-PCF (p-PCF) function at ANG (in WLAN IP network) implements the R-P interface in order to communicate to the PDSN.
- An Access Router (AR) discovers and selects a p-PCF in WLAN IP network and tunnels PPP frames from the MS served by its APs to the p-PCF.

Note that the cdma2000 standard allows two modes of IP access; Simple and Mobile IP mode. The Integrated network architecture is transparent to the cdma2000 IP access mode and works well for both methods.

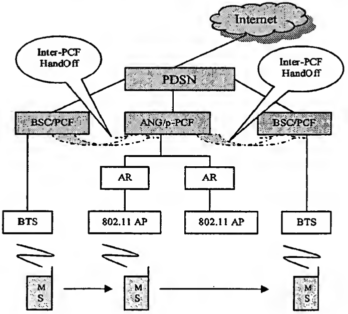


Figure 3. Integrated Network Architecture

In the following sections, we explain the ways in which various access and network operations are supported in the integrated network architecture.

IV. ACCESS AUTHENTICATION

A. *CDMA2000 Network*

Two levels of security are provided in the cdma2000 network. In the first level of security, the mobile device is authenticated and authorized by mobile switching center (MSC) through the home location register (HLR) and visitor location register (VLR) databases. This is performed prior to

granting access to the radio network for packet data service. In the IP network access security mode, the mobile user is authenticated and authorized using standard authentication, authorization and accounting (AAA) [20] protocol via PDSN. This step is performed prior to granting access to the IP network.

B. 802.11 WLAN Network

The 802.1x protocol enables access authentication through the 802.11 WLAN access network. This protocol allows the mobile stations (MS) to be authenticated via the access points and vice versa. 802.1x takes advantage of an existing authentication protocol known as the Extensible Authentication Protocol (EAP) [17]. The 802.1x authentication for wireless LANs has three main components: The supplicant (usually the client software in the MS); the authenticator (usually the access point); and the authentication server (usually a Remote Authentication Dial-In User Service server). At the end of the 802.1x transactions, the goal of authenticating the mobile stations by the 802.11 network is completed, enabling the access point port for uninhibited access by the end station. However, this leaves the access point open to attacks by a rogue mobile station that can spoof the identity of the authorized station. The Robust Secure Network Association (RSNA) [19] protocol being standardized by IEEE 802.11i allows for packets between the access point and end station to be encrypted and signed. RSNA uses advanced cryptographic technologies (TKIP, AES) to provide a higher level of security. Once the RSNA exchange has been completed, the end station and the access point have shared secret keys that can be used to encrypt and sign subsequent packets. This allows the access point to indeed ensure that only the authenticated user is using the ports.

V. IP ADDRESS MANAGEMENT

The cdma2000 and the WLAN networks may use subnet IP domains that are topologically distinct. At the PDSN, the routing of the IP traffic to/from the MS is performed based on the IP address assigned to the MS by the PDSN during the PPP/IPCP negotiation phase. This address may not be topologically correct when the MS is attached to the WLAN network which may cause the forwarding of IP packets to/from the MS to fail.

The integrated architecture assigns a separate IP transport address to the MS that is used within the WLAN network to route the packets to the AR that is currently serving the MS. This address must be assigned only once when the MS first gets attached to the WLAN network and is not changed as long as the MS is moving within WLAN access network. The AR to which the MS first gets attached in the WLAN network provides or requests this IP address on behalf of the MN -- this address is not visible to the MS itself. The micro-mobility solution used within the WLAN is transparent to the MS and uses this IP transport address to forward packets to/from MS within WLAN network.

VI. MOBILITY

A. Mobility across cdma2000 Technology

Three levels of mobility support are provided in the cdma2000 architecture:

The first level of mobility is at the sector/sector or cell/cell level [5] within the domain of a PCF. This level of mobility is handled at the radio link layer and is hidden from the PDSN and from higher level mobility functions (e.g. Mobile IP foreign agent (FA) and home agent (HA)).

The second level of mobility is across PCF domains within the scope of a PDSN. This is handled by the PDSN because it can be logically connected to more than one PCF. This level of mobility is referred to as "R-P Mobility" or "intra-PDSN Mobility". The R-P interface for a session can be moved from one PCF to the other in such a way that it is transparent to the PPP session running between the MS and the PDSN. Because the PPP session remains on the same PDSN, that session is kept intact and the MS does not need to renegotiate PPP, LCP or IPCP options.

The highest level of mobility in cdma2000 is available only when the PDSN incorporates a Mobile IP Foreign Agent (FA) which allows mobility with respect to the connection point to the Internet to be anchored at the Home Agent (HA). This level of mobility is described as "Macro-Mobility" and allows inter-PDSN mobility to occur. If the mobility handoff results in an connection to a new PCF that does not have access to the old PDSN/FA (inter-PDSN mobility), a new PPP session must be established. When using Mobile IP, the PDSN/FA is informed that a new PPP session is active and the PDSN/FA issues an Agent Advertisement on that session. The mobile responds with a Registration Request which the PDSN/FA forwards to the HA.

B. Mobility Support across WLAN Technology

The Inter Access Point Protocol (IAPP) [10] controls the mobility across APs connected through the same AR (an intra-AR handover).

An inter-AR handover, using IP-based micro-mobility mechanisms, is required when the APs involved in the handover are connected to different ARs. The mobile does not change its IP address during the course of its association and de-association with different APs. There are currently no standards in this area, however there are a number of proposed protocols that attempt to solve the local mobility of mobile [12, 13, 14, 15, 16]; the mechanism described earlier under "IP Address Management" is another one of these approaches.

C. Inter-Technology Handover with 'PCF-Peering'

The point-to-point protocol (PPP) is the standard mechanism for packet data transport in a cdma2000 network. In order to perform a seamless handoff of the cdma2000 data session, the PPP state must be kept up and running at the two PPP endpoints (MS and the PDSN) before, during and after the handoff. If the PPP session is broken, it takes a minimum of 9 and a maximum of 15 messages between the MS and the PDSN to (re-) negotiate a PPP session. This includes the link

layer, authentication, and network layer negotiation phases, all of which must be re-done if the PPP session is broken; it does not include possible additional messages due to dropped or damaged packets over the air.

As mentioned in previous sections, R-P mobility (Intra-PDSN, Inter-PCF handover) mechanism of the CDMA2000 standard supports the mobility between the PCFs without breaking the PPP session between the MS and the PDSN. The handoff between the two PCFs is performed as a layer 2 handoff while the upper layer states (like the PPP state) remain unchanged. We propose a "PCF-Peering" mechanism that re-uses the concept of inter-PCF, intra-PDSN (R-P mobility) to perform the seamless mobility between cdma2000/ WLAN technologies. The "proxy-PCF" functionality is introduced in the WLAN access network gateway (ANG) which connects the WLAN access network with the cdma2000 PDSN. The WLAN access network is hidden behind this Proxy PCF and appears as a cdma2000 radio access network to the PDSN. The PPP data is transported through the GRE-based interface between the proxy PCF and the PDSN while the data transport between the proxy PCF and the AP still uses the inherited micro mobility and link layer mechanisms of the wireless technology to set up the data transport. Figure 4 presents the network architecture for the integrated cdma2000-WLAN access network with PCF-Peering concept.

1) General Scenarios

Following are the four main scenarios that can be discussed to explain the integrated architecture:

a) MS powers up in cdma2000 network and establishes PPP session with PDSN
b) MS handovers from the WLAN access to cdma2000 access with pre-established PPP state
c) MS powers up in WLAN access networks and establishes PPP state with PDSN
d) MS handovers from the cdma2000 access network with pre-established PPP state

Scenarios (a) and (b) follow the standard cdma2000 procedures described in [6] and are not described further in this document. The following sections capture scenario (c), the power up in 802.11 WLAN access network, and scenario (d), handover from cdma2000 access network to 802.11 access network. Figures 5 and 6 describe the high level interactions between various network elements for power up and handover, scenarios (c) and (d) respectively. In both cases, the communication between the ANG (where p-PCF function resides) and the PDSN follows the cdma2000 standard A11 signalling procedures [6].

2) MS Powers up in WLAN

In scenario (c), during power up in WLAN access network, MS uses the IP address assigned to the MS by the PDSN during the PPP establishment phase to communicate with the AR. However, the routing of IP traffic between the AR and ANG is performed using the WLAN transport address assigned to the MS by the AR during the association phase.

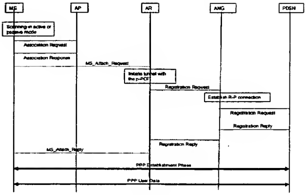


Figure 4. MS Power up in WLAN Procedures

3) Cdma2000 to WLAN Handoff

In scenario (d), when the WLAN air interface of the MS detects strong WLAN coverage while having pre-established data sessions (and hence the PPP state at the PDSN) via cdma2000 access network, it re-uses the PDSN assigned IP address when it attaches to the WLAN network. An inter-PCF handover is performed (between the PCF at cdma2000 BSC and the p-PCF at the WLAN ANG) and the MS continues sending/receiving IP traffic via the WLAN access network. No PPP (re-)establishment is required in this scenario. Once again, the routing of IP traffic between the AR and ANG is performed using the WLAN transport address assigned to the MS by the AR during the association phase.

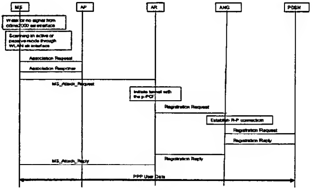


Figure 5. CDMA2000-to-WLAN Handoff Procedures

VII. Packet Transport

The packet transport in the integrated network uses PPP framing between the MS and the PDSN as defined by the cdma2000 standard.

However, the following modes of packet transport are used across WLAN network.

- Layer 2 end points of the data transport are the MS and the AR. The data transport mechanism uses raw encapsulation of PPP packets inside 802.11/Ethernet frames [1]. The MS transmits/receives the PPP data encapsulated in 802.11 frames to/from the AP. The AR transmits/receives the PPP data encapsulated in Ethernet frames.
- Tunneled (PPP-in-IP) transport of the PPP data is used between AR and the ANG/Proxy-PCF.
- Tunneled (PPP-in-GRE) transport of the PPP data is used over the R-P interface.

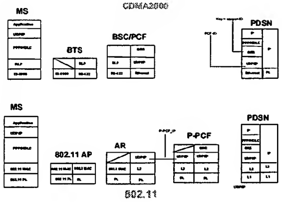


Figure 6. Bearer plane protocol stacks

VIII. Accounting

Since the PCF-peering mechanism re-uses the R-P mobility concept, the proposed architecture does not require any special mechanism to enable the accounting/charging during handoffs between the cdma2000 and WLAN access networks. The current standard supports mechanisms to inform the AAA server when an R-P interface is moved.

IX. Conclusion

In this paper, we presented the unique concept of "PCF-peering" that can be applied to perform seamless handoffs between the 3G cdma2000 and WLAN access technologies. The paper explains the proposed network architecture and the functions that are required at various network elements. The main advantage of the PCF-peering concept is that it uses the existing cdma2000 mobility management mechanisms to handle the handoffs between cellular and WLAN access technologies. The handoff is performed at layer 2 so that the upper layers are not even aware of the change of radio interface. This concept does not require any changes to the existing cdma2000 radio/network standards nor to the WLAN radio standard, allowing it to be introduced into existing cdma2000 and 802.11 networks.

[1] PPP encapsulation over Ethernet is different from PPPoE and is not a standard mechanism as yet

Acknowledgements

Special thanks to the WTL development team (Peter Hazy, Kris Ng, Eugenia Lambiri, Goran Janevski, and Biswaroop Mukerjee) for turning the concepts into a working test bed with live cdma2000 and 802.11 WLAN air interfaces.

References

[1] *M. Jaseemuddin*, An Architecture for Integrating UMTS and 802.11 WLAN Networks, accepted to appear in the proceedings of IEEE Symposium on Computers and Communications (ISCC2003), Antalya, Turkey, June 30 - July3 2003.

[2] A. Salkintsiz, C. Fors, and R. Pazhyannur, WLAN-GPRS Integration for Next generation Mobile Data Networks, IEEE Wireless Communications, pp. 112-124, October 2002.

[3] J. Ala-Laurila, J. Mikkonen, and J. Rinnemaa, Wireless LAN Acce Network Architecture for Mobile Operators, IEEE Communications, pp. 82-89, Vol. 39, No. 11, November 2001.

[4] BRAN HIPERLAN 2: Requirements and Architectures for Interworking between HIPERLAN/2 and 3rd Generation Cellular Systems, ETSITR 101 957 V11.1.1, www.etsi.org, June 2001.

[5] Cdma2000 Wireless IP Network Standard. http://www.arib.or.jp/IMT-2000/ARIB-spec/ARIB/P.S0001.PDF.

[6] Interoperability Specification (IOS) for CDMA2000 Access Network Interfaces - Part 7 (A10 and A11 Interfaces). Revision 0 (3G IOSv4.2). http://www.3gpp2.org/Public_html/specs/index.cfm

[7] Wireless LAN802.11 Standard. http://grouper.ieee.org/groups/802/11/

[8] IEEE Std. 802.11b, Supplement to ANSI/IEEE Std. 802.11, 1999 Edition, IEEE Standard for Wireless LAN MAC and PHY Specifications, PDF: ISBN 0-7381-1812-5, January 2000.

[9] Mathew Gast, 802.11 Wireless Networks- The Definitive Guide, O'Reilly, 2002.

[10] IEEE 802.11f standard: Recommend Practice for Multi-Vendor Access Point Interpretability via an Inter-Access Point Protocol. http://grouper.ieee.org/groups/802/11/private/Draft_Standards/11f/802.11f-D3.1.pdf.

[11] W. Simpson, "The Point-to-Point Protocol (PPP)", July 1994, RFC 1661. http://www.ietf.org/rfc/ rfc1661.txt?number=1661.

[12] R.Ramjee, et. al., "IP micromobility support using HAWAI", IETF Draft, July 2000. http:// search.ietf.org/internet-drafts/draft-ietf-mobileip-hawaii-o1.txt

[13] A. Campbell et. al., "Cellular IP", IETF Draft, January 2000. Http://search.ietf.org/internet-drafts/ draft-ietf-mobileip-cellularip-00.txt

[14] A. Campbell, J. Gomez, S. Kim, A. Valko, C. Wan, Z. Turanyi, Design, Implementation, and Evaluation of Cellular IP, IEEE Personal Communications, Vol 7, No. 4, pp. 42-49, August 2000.

[15] H. Soliman, C. Castelluccia, K. Elmalki, L. Bellier, Hierarchical Mobile IPv6 Mobility Management, Internet Draft, draft-ietf-mobileip-hmipv6-07.txt, October 2002.

[16] Hongyi Li, et.al., "Mobile Routing for Large Scale Wireless Internet," in Mobile Computing and Communication Review, vol. 4, No.4, pp. 36-44, 2000.

[17] L. Blunk et. al., "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998. http:// www.ietf.org/rfc/rfc2284.txt?number=2284.

[18] S. Hanks et al., "Generic Routing Encapsulation (GRE)", RFC 1701, Oct. 1994. http://www.faqs.org/rfcs/rfc1701.html.

[19] D. Halasz, "IEEE802.11i Draft and Call for Interest on Link Security for IEEE 802 Networks", November 2002. http://www.ieee802.org/linksec/meetings/MeetingsMaterial/Nov02/halasz_sec_1_1102.pdf.

[20] The IETF Authentication, Authorizartion and Accounting WG Home Page. http://www.ietf.org/html.charters/aaa-charter.html